DOI: 10.18372/2310-5461.63.19754
УДК 004.622: 517.927

Д. В. Бараннік
Харківський національний університет радіоелектроніки
orcid.org/0000-0002-7074-9864
e-mail: d.v.barannik@gmail.com;

МЕТОД ЗМІШАНОГО СТЕГАНОКОМПРЕСІЙНОГО КОДУВАННЯ В ПОЗИЦІЙНО-ПОЛІАДИЧНОМУ БАЗИСІ

Вступ

В сучасних умовах край важливим є забезпечення умов для ефективного: застосування та всебічної підтримки Сил оборони та безпеки України; функціонування критичної інфраструктури держави. В загалі це є комплексним питанням. Водночас одним з найважливіших аспектів є досягнення відповідних вимог в процесі організації відеоінформаційного забезпечення та політики інформаційної безпеки [1–3]. Тут розуміється створення та надання таких інформаційних сервісів, за умов використання яких з врахуванням питань кібербезпеки досягаються можливості щодо: інформаційної переваги в процесі управління підрозділами та об'єктами Сил оборони та безпеки України (СОБУ); підвищення ефективності процесів аналізу та прийняття рішень в системах управління критичною інфраструктурою; належного рівня інформування соціуму; організації конструктивного інформаційного простору на міжнародній арені, наприклад інформаційної взаємодії з країнами-партнерами [4; 5].

Тут потрібно враховувати те, що відеоінформаційні ресурси *одночасно* можуть мати два функціональних призначення, а саме як [6; 7]:

1) значуща інформація з позиції ключового впливу на ефективність аналізу та прийняття рішень в КРІС та ОСД;

2) контейнерів для приховування спеціальних відомостей в системах комплексного захисту інформації.

Подалі відеоінформаційні ресурси подвійного призначення позначатимемо значимими відеоконтейнерними ресурсами (ЗВКР).

Актуальність та критичність забезпечення конфіденційності (спеціальної) інформації з використанням етапу формування та/або передачі бортовими інфокомунікаційними системами в умовах воєнного стану зумовлено [8–10]:

1) з одного боку наявністю наступних потенціалів для протиборчої сторони [11; 12]:

– можливостей для протиборчої сторони щодо: перехвату інформації під час її передачі по радіоканалам з бортових комплексів; перехвату управління безпілотною платформою; деструктивних дій, які призводять до втрати подальшої можливості щодо виконання бортовим комплексом своїх функціональних завдань;

– інформаційно-технологічних можливостей щодо спроби реалізації несанкціонованого доступу до інформаційного ресурсу, в тому числі проведення кібернетичних атак та крипто-аналізу для розкриття змісту конфіденційної інформації;

- можливості доступу до інформаційних технологій загального користування щодо: дистанційного відео-контролю (ВКОН) через сенсорні пристрої; відеоконференцзв'язку (ВКЗ) через загальнодоступні технології обміну інформацією;

– можливості використовувати вразливі фактори в системах забезпечення інформаційної безпеки, в тому числі техногенного та антропогенного походження.

– можливості вживання спеціальних технічних засобів в технологічних пристроях, які використовуються в якості мікроелектронної основи для інтегрування (реалізації) алгоритмів обробки та криптографічного захисту інформації;

2) з іншого боку наявністю множини вразливих факторів в процесі організації доставки та захисту інформаційного ресурсу бортовими інфокомунікаційними технологіями (БІКТ): наявністю нормативно-законодавчих обмежень щодо сертифікації та впровадження вітчизняних засобів криптографічного захисту інформації; наявністю використання незахищених каналів зв'язку; використанням форматів представлення та передачі даних закордонного виробництва; обмеженість пропускної спроможності бортових інфокомунікаційних систем щодо обробки та передачі даних [13; 14].

Отже актуальною ***науково-прикладною задачею*** є підвищення інформаційної безпеки за умов надання потрібного рівня відеоінформаційного забезпечення з використанням безпілотних платформ.

Постановка проблеми

Конфіденційність в загальному випадку може забезпечуватись комплексним підходом. Для цього залучаються технології криптографічного захисту та стеганографічних перетворень (СТП). Водночас збільшується актуальність та значимість застосування СТП [15–18].

В той же час для сучасних варіантів сумісного послідовного використання стеганографічних та компресійних перетворень існують такі недоліки [19; 20]:

– збільшуються втрати за рівнем стиснення $\Delta\vartheta^{(k,\ell)} < 1$ (оскільки порушуються структурно-семантичні залежності для трансформованого ВС). В залежності від рівня інформативності ВС та режиму квантування втрати рівня стиснення можуть сягати від 10 до 70 %;

– значно зменшується рівень ПВСШ, тобто $\rho_{steg}^{(k,\ell)} < \rho_{nes}$. Це вказує на: втрату цілісності ЗВКР; демаскування факту наявності прихованої у ВС інформації;

– за умов зменшення втрат рівня стиснення та збільшення семантичної цілісності ВСС за показником $\rho_{steg}^{(k,\ell)}$ відбувається падіння рівня стеганографічної ємності в 4 рази.

Звідси існуючи методи СТП не забезпечують вимог за показниками: швидкості прихованого у кодованому відеопотоці каналу вбудованих повідомлень; стеганографічної ємності; обмеження впливу на ефективність компресійного кодування; цілісність вилученої на приймальній стороні прихованої інформації; демаскування факту наявності вбудованих до ВС прихованих повідомлень.

Таким чином, мета досліджень статті полягає у необхідності підвищення ефективності стеганографічних перетворень в процесі передачі стиснутого (кодованого) відеопотоку інфокомунікаційними мережами для заданих властивостей відеосервісів з використанням бортових ІКС.

Обґрунтування вимог до стенографічних перетворень в умовах забезпечення оперативності та цілісності доставки відеоконтейнерних ресурсів безпроводовими інфокомунікаційними мережами

Бортові відеоресурси, для яких передбачається встановлення значимих фрагментів, як спеціальної інформації, що потрібує захисту, є достатньо інформативними за структурно-семантичним змістом. В цьому випадку кількість відеосегментів, що потребують захисту (приховуванню) сягає в середньому від 10 до 30 % від їх загальної кількості у відеокадрі (аерофотознімку). Звідси:

– формуються (визначаються) можливі вимоги до $10 \le R_{steg,nes\%}^{(k,\ell)} \le 30\,\%$ та кількості $\nu(\hbar_{clr})_{hid,nes}$ вбудованих біт в реальному часі, $\nu(\hbar_{clr})_{hid} = R_{steg}^{(k,\ell)} \cdot V(\nu_s)$: HD (720p) (1280×720) – $2{,}2 \le \nu(\hbar_{clr})_{hid,nes} \le 7$ Мбіт; Full HD (1920×1080) – – $4{,}8 \le \nu(\hbar_{clr})_{hid,nes} \le 14{,}5$ Мбіт; 4K Ultra HD HV (3840×2160) - $19 \le \nu(\hbar_{clr})_{hid,nes} \le 60$ Мбіт; 4K UHD; (4128×3096) – $30 \le \nu(\hbar_{clr})_{hid,nes} \le 90$ Мбіт; 8K (8192×3357) – $96 \le \nu(\hbar_{clr})_{hid,nes} \le 290$ Мбіт;

– висувається потреба у вилучені інформації на приймальній стороні або з потрібним рівнем семантичної цілісності $\rho_{hid}^{(k,\ell)}$, $\rho_{hid}^{(k,\ell)} \ge \rho_{nes}$ (ПВСШ $\rho_{hid}^{(k,\ell)}$, як для високоінформативних ВС) або без втрат синтаксичної цілісності, тобто $\sigma_{hid}^{(k,\ell)} \to 0$ (або ймовірність $P_{hid}^{(k,\ell)}$ безпомилкового вилучення інформації дорівнює 1, $P_{hid}^{(k,\ell)} \to 1$), у разі якщо значимий ВС був попередньо стиснутий (тобто тут вже враховані допустима кількість ПСВ надмірності).

Обґрунтування потреби щодо узагальнення показників оцінювання ефективності сумісного використання стеганографічних та компресійних перетворень

В якості показника оцінювання ефективності СТП в умовах компресійного кодування ЗВК ресурсів для передачі бортовими ІКТ пропонується застосовувати швидкість S_{hid} прихованого у компресійному відеопотоці каналу передачі спеціальних (вбудованих) повідомлень. Складовими показника S_{hid} є:

– швидкість S_{ch} передачі даних в інфокомунікаційному каналі (або сегментована швидкість ${}_{\Delta}\mathrm{S}_{\mathrm{s}}$, ${}_{\Delta}S_s = S_{ch} / I(n;b) = S_{ch} / 8 \cdot n \cdot n$);

– рівень $\vartheta_{steg}^{(k,\ell)}$ стиснення з врахуванням процесу вбудовування інформації:

$$\vartheta_{steg}^{(k,\ell)} = V_{beg}^{(k,\ell)} / V_{steg}^{(k,\ell)} = \\ = I(n;b) / V_{steg}^{(k,\ell)} = \hbar_{sp} \cdot \hbar_{px} / V_{steg}^{(k,\ell)} \quad (1)$$

– значення $R_{steg}^{(k,\ell)}$ стеганографічної ємності відносно початкового бітового об'єму послідовності ВС.

Це дозволяє врахувати особливості стеганографічних та компресійних перетворень на швид-

кість передачі відеоданих з прихованою інформацією.

Відповідно до чого маємо наступні співвідношення:

1) швидкість S_{steg} відео каналу з прихованою інформацією з врахуванням сегментоорієнтовної обробки ЗВК ресурсів:

$$S_{steg} = \nu_s \cdot S_{ch} \; / \; \sum_{\tau=1}^{\nu_s} \frac{I(n;b)}{\vartheta_{steg}^{(\tau)}} = \\ = \nu_s \cdot \left({}_{\Delta}S_s \; / \left(\sum_{\tau=1}^{\nu_s} \frac{1}{\vartheta_{steg}^{(\tau)}} \right) \right) (\text{сег/с}); \quad (2)$$

2) показник S_{hid}

$$S_{hid} = \nu_s \cdot S_{ch} \; / \; \sum_{\tau=1}^{\nu_s} \frac{I(n;b)}{R_{steg}^{(\tau)} \cdot \vartheta_{steg}^{(\tau)}} = \\ = \nu_s \cdot \left({}_{\Delta}S_s \; / \left(\sum_{\tau=1}^{\nu_s} \frac{1}{R_{steg}^{(\tau)} \cdot \vartheta_{steg}^{(\tau)}} \right) \right) (\text{сег/с}). \quad (3)$$

В співвідношеннях (2), (3) для спрощення двовимірні координати $(k;\ell)$ ВС замінюються одновимірною τ.

У разі, якщо рівень стиснення та стеганографічної ємності не має значимих змін в послідовності ВС, то можна використовувати відповідно усереднені значення $\overline{\vartheta}_{steg}$ та $\overline{R}_{steg}$:

$$\overline{\vartheta}_{steg} = \left(\sum_{\tau=1}^{\nu_s} \vartheta_{steg}^{(\tau)} \right) / \nu_s ; \; \overline{R}_{steg} = \left(\sum_{\tau=1}^{\nu_s} R_{steg}^{(\tau)} \right) / \nu_s .$$

Тоді співвідношення для S_{hid} виглядатиме:

$$S_{hid} = \overline{R}_{steg} \cdot \overline{\vartheta}_{steg} \cdot {}_{\Delta}S_s \; (\text{сег/с}). \quad (4)$$

Розробка напрямку створення нових інфокомунікаційних технологій в сфері стеганографічних та ком прерійних перетворень

В основі проблемних недоліків сучасних стеганографічних систем на концептуальному рівні їх створення лежить наступне *системне протиріччя:*

1. З одного боку існуючі ІКТ кодування створюються без попереднього врахування можливості прихованого вбудовування повідомлень. Тобто в процесі побудови технологічних етапів трансформації та кодування не закладається можливість поточних модифікацій синтаксичного опису, який описує психовізуальні, статистичні та структурні залежності у ВС.

2. З іншого боку теоретична база сучасних стеганографічних перетворень не в повній мірі враховує технологічні особливості процесів скорочення кількості надмірності та кодування.

Для локалізації означеного системного протиріччя *пропонується* створювати двохситуаційну технологічну платформу кодування послідовності ВС. Вона включатиме до себе метод компресійного кодування ВС з вбудовуванням прихованої інформації з наступними технологічними характеристиками: локалізувати взаємний деструктивний вплив між стеганографічними та компресійними перетвореннями; зменшити долю кількості ПСВ надмірності в результуючому рівні стиснення ВС та стеганографічної ємності вбудованих даних; забезпечити в процесі компресії та СТП врахування структурно-комбінаторних залежностей для ВС та їх перехідних форматів; створити підходи щодо вбудовування прихованої інформації безпосередньо в динаміці реалізації процесу кодування та створення поточного формату ВС; адаптуватися за рівнем скорочення кількості надмірності та об'єму вбудованих даних відповідно до визначеного рівня СТС інформативності ВС.

Звідси необхідно розробки методу стеганокомпресійних перетворень для підвищення швидкості прихованого у кодованому відеопотоці каналу вбудованої інформації на основі врахування інформативності та структурних залежностей у відео сегменті-контейнері.

Розробка змішаного стеганокомпресійного кодування

З врахуванням процесу форматування РСПБ пропонується наступне уточнення поняття СК-кодування. Процес побудови кодового значення з одночасною прихованою імплантацією доданого елементу в стегано-поліадичному базисі на основі встановлення та скорочення кількості ППК надмірності називається *стеганокомпресійне (СК) кодування в розширеному поліадичному базисі*.

В цьому разі елемент $g(u)_{\chi}$ послідовності G_u додається на другу позицію α-го ППЧ $A(\alpha)_j^{(k,\ell)}$ для j-го стовпця ВСК $A^{(k,\ell)}$, тобто $\tilde{A}'(\alpha)_j^{(k,\ell)} = g(u)_{\chi} \bigcup A(\alpha)_j^{(k,\ell)} \mid \tilde{a}'(\alpha)_{2,j}^{(k,\ell)} = g(u)_{\chi}$.

Маємо такий вигляд стегано-ППЧ $\tilde{\mathrm{A}}'(\alpha)_{\mathrm{j}}^{(\mathrm{k},\ell)}$ в розширеному СПБ $\tilde{\mathrm{Q}}'(\alpha)^{(2,\mathrm{k},\ell)}$:

$$\tilde{A}'(\alpha)_j^{(k,\ell)} = \{ a(\alpha)_{1,j}^{(k,\ell)}; \; g(u)_{\chi}; \\ a(\alpha)_{2,j}^{(k,\ell)}; ..; a(\alpha)_{i,j}^{(k,\ell)}; ...; a(\alpha)_{n_{\alpha},j}^{(k,\ell)} \} . \quad (5)$$

Відповідно необхідно будувати такий базис $Q(\alpha)^{(2,k,\ell)}$:

$$\tilde{Q}'(\alpha)^{(2,k,\ell)} : \; (\tilde{q}'(\alpha)_{2,j}^{(k,\ell)} + 1) \bigcup Q(\alpha)^{(2,k,\ell)} .$$

Відповідно позиційно-комбінаторна вага $\widetilde{\mathrm{w}}'(\alpha)_{\mathrm{i,j}}^{(\mathrm{k},\ell)}$ для зворотно-залежного процесу розраховується наступним чином (для такого варіанту позиція вбудованого елементу $\mathrm{g(u)}_{\chi}$ визначається, як $\tilde{a}'(\alpha)_{2,j}^{(k,\ell)} = g(u)_{\chi}$):

$$\tilde{w}'(\alpha)_{i,j}^{(k,\ell)} = (\tilde{q}'(\alpha)_{2,j}^{(k,\ell)} + 1)^{sign(1+sign(1-i))} \times \times \prod_{\xi=i+1}^{n_\alpha+1} \left(q(\alpha)_{\xi,j}^{(k,\ell)} + 1\right). \quad (6)$$

Імплементація доданого елементу $\mathrm{g(u)}_{\chi}$ до стеганокомпресійної (СК) кодограми здійснюється за допомогою позиційного кодування СППЧ в РСПБ $\widetilde{\mathrm{Q}}'(\alpha)^{(2,\mathrm{k},\ell)}$. Для цього застосовується загальна формула:

$$\widetilde{\mathrm{N}}'(\alpha)_{\mathrm{j}}^{(\mathrm{k},\ell)} = \sum_{\mathrm{i}=1}^{\mathrm{n}_\alpha+1} \widetilde{\mathrm{a}}'(\alpha)_{\mathrm{i,j}}^{(\mathrm{k},\ell)} \cdot \widetilde{\mathrm{w}}'(\alpha)_{\mathrm{i,j}}^{(\mathrm{k},\ell)}.$$

Потрібно враховувати залежність від напрямку процесу визначення ваги $\tilde{w}'(\alpha)_{i,j}^{(k,\ell)}$. Для зворотно-залежного процесу визначення ваги з врахуванням співвідношення:

$$\tilde{a}'(\alpha)_{i,j}^{(k,\ell)} = sign(1-|sign(i-2)|)\cdot g(u)_{\chi} + +|sign(i-2)|\cdot a(\alpha)_{i-sign(1+sign(i-2)),j}^{(k,\ell)}$$

матимемо:

$$\tilde{N}'(\alpha)_{j}^{(k,\ell)} = g(u)_{\chi}\cdot\tilde{w}'(\alpha)_{2,j}^{(k,\ell)} + + \sum_{i=1}^{n_\alpha+1} |sign(i-2)|\cdot a(\alpha)_{i-sign(1+sign(i-2)),j}^{(k,\ell)})\times \cdot \quad (7) \times \tilde{w}'(\alpha)_{i,j}^{(k,\ell)}$$

В створених формулах використовуються такі позначення: $\tilde{N}'(\alpha)_{j}^{(k,\ell)}$ - кодове значення стеганопослідовності $\tilde{A}'(\alpha)_{j}^{(k,\ell)}$ або стегано-кодове значення для α-ї складової j-го стовпця $(k;\ell)$-го ВС у разі врахування ППК залежностей.

Процес формування кодового значення для ППЧ з використанням виразів (5)-(7) визначається, як *стеганокомпресійне кодування в розширеному стеганополіадичному базисі*.

Відповідно процес інтеграції доданого біту прихованого повідомлення в процесі формування кодового значення на основі позиційного кодування в поліадичному базисі визначається, як *стеганокомпресійна імплементація в розширеному стеганополіадичному просторі*.

Процес стеганокомпресійного кодування завершується етапом формування відповідного двійкового синтаксичного опису $\tilde{C}'(\alpha)_{j}^{(k,\ell)}$ для стегано-кодового значення $\tilde{N}'(\alpha)_{j}^{(k,\ell)}$ послідовності $\tilde{A}'(\alpha)_{j}^{(k,\ell)}$. Створення такого опису з вбудованою інформацією організується на основі побудови відповідної СК-кодограми $\tilde{C}'(\alpha)_{j}^{(k,\ell)}$. Це необхідно здійснювати з врахуванням ППК залежностей $\tilde{Q}'(\alpha)^{(2,k,\ell)}$.

Тут потрібно враховувати величину обмежень $\tilde{W}'(\alpha)_{j}^{(k,\ell)}$ на стегано-кодове значення $\tilde{N}(\alpha)_{j}^{(k,\ell)}$, тобто:

$$\tilde{W}'(\alpha)_{j}^{(k,\ell)} = \prod_{i=1}^{n_\alpha+1} \left(sign(1+\delta)\cdot q(\alpha)_{j}^{(k,\ell)} - -\delta\cdot sign(1-\delta)\cdot\tilde{q}'(\alpha)_{i}^{(k,\ell)} + 1\right). \quad (8)$$

Отже величина $\tilde{W}'(\alpha)_{j}^{(k,\ell)}$ встановлює об'єм множини $\tilde{\Omega}'(\alpha)_{j}^{(k,\ell)}$ допустимих СППЧ $\tilde{A}'(\alpha)_{j}^{(k,\ell)}$, які утворюються за умов виконання обмежень $\tilde{q}'(\alpha)_{i,j}^{(k,\ell)}$ на їх елементи $\tilde{a}'(\alpha)_{i,j}^{(k,\ell)}$, $\tilde{a}'(\alpha)_{i,j}^{(k,\ell)} \in \tilde{A}'(\alpha)_{j}^{(k,\ell)}$, для $i = \overline{1,\,(n/\alpha)+1}$. Тобто:

$$\tilde{a}'(\alpha)_{i,j}^{(k,\ell)} \le \tilde{q}'(\alpha)_{i,j}^{(k,\ell)} = sign(1+\delta)\cdot q(\alpha)_{j}^{(k,\ell)} - -\delta\cdot sign(1-\delta)\cdot q(\alpha)_{i}^{(k,\ell)}. \quad (9)$$

Співвідношення (8) дозволяє визначити кількість $\tilde{v}(\alpha)_{j}^{(k,\ell)}$ біт на представлення стегано-кодового значення $\tilde{N}'(\alpha)_{j}^{(k,\ell)}$ з виключенням додаткової інформації за умов виконання нерівності (9) щодо унеможливлення переповнення кодограми. Для цього задіється формула:

$$\tilde{v}(\alpha)_{j}^{(k,\ell)} = \left\lceil \sum_{i=1}^{n_\alpha+1} \ell og_2(sign(1+\delta)\cdot q(\alpha)_{j}^{(k,\ell)} - -\delta\cdot sign(1-\delta)\cdot q(\alpha)_{i}^{(k,\ell)} + 1)\right\rceil + +sign\left(\tilde{W}'(\alpha)_{j}^{(k,\ell)} \bmod(2^{\beta})\right). \quad (10)$$

Процес імплементації вбудованого елементу в процесі компресійних перетворень до двійкового синтаксичного опису через відповідне розміщення стегано-кодового значення на основі блокового двійкового декодування позначатимемо, як *СК імплементація прихованої інформації на двійковому синтаксичному рівня СК представлення*.

Імплементація доданого біту здійснюється в умовах його поліадизації (вростанням до поліадичного базису). Тому СК-перетворення за виразами (6) та (8)–(10) забезпечує виключення втрат синтаксичної цілісності контейнера та прихованих повідомлень.

Після побудови стегано-кодового значення $\tilde{N}'(\alpha)_j^{(k,\ell)}$ та його розміщення в синтаксичному описі $\tilde{C}'(\alpha)_j^{(k,\ell)}$ СК-представлення необхідно провести завершальний етап стеганокомпресійних перетворень. Потрібно організувати маскування РСПБ $\tilde{Q}'(\alpha)^{(2,k,\ell)}$ з одночасним непрямим вбудовуванням додаткового $(\chi+1)$-го елементу $g(u)_{\chi+1}$ прихованого повідомлення G_u. Для цього потрібно створити змішано-маскований базис (ЗМПБ) $\hat{Q}''(\alpha)^{(2,k,\ell)}$. Побудова такого базису здійснюється з врахуванням правилу змішаного маскування, що задається системою:

$$(\hat{q}''(\alpha)_{i,j}^{(k,\ell)}+1)=\begin{cases}(\hat{q}''(\alpha)_{1,j}^{(k,\ell)}+1)=\\ =\lambda\cdot((q(\alpha)_{1,j}^{(k,\ell)}+1)+g(u)_{\chi+1}),\\ \quad\to i=1;\\ (q(\alpha)_{i,j}^{(k,\ell)}+1),\\ \to 2\le i\le n_\alpha;\end{cases}$$

особливостей форматування РСПБ базису, відповідно до системи співвідношень:

$$(\tilde{\mathrm{q}}'(\alpha)_{\mathrm{i,j}}^{(\mathrm{k},\ell)}+1)=\begin{cases}(\mathrm{q}(\alpha)_{\mathrm{1,j}}^{(\mathrm{k},\ell)}+1), & \to \mathrm{i}=1;\\ (\tilde{\mathrm{q}}(\alpha)_{\mathrm{2,j}}^{(\mathrm{k},\ell)}+1)=2, & \to \mathrm{i}=2;\\ (\mathrm{q}(\alpha)_{\mathrm{i-1,j}}^{(\mathrm{k},\ell)}+1), & \to 3\le \mathrm{i}\le \mathrm{n}_\alpha+1.\end{cases}$$

Відповідно до чого за умов $w(\alpha)_{i,j}^{(k,\ell)}\uparrow$ для $i\downarrow$ потрібно корегувати ПОБ першої компоненти ППЧ, тобто:

$$\hat{q}''(\alpha)_{1,j}^{(k,\ell)}+1=2\cdot((q(\alpha)_{1,j}^{(k,\ell)}+1)+g(u)_{\chi+1}.$$

Тут $\hat{q}''(\alpha)_{1,j}^{(k,\ell)}$ - перша компонента базису $\hat{Q}''(\alpha)^{(2,k,\ell)}$.

Висновки

Створено метод змішаного стеганокомпресійного кодування на основі позиційно-поліадичного базису з маскуванням. Базові характеристики методу полягають у: створені стеганокомпресійних перетворень в змішано-маскованому базисі; реалізації двокаскадної ***кодово-компресійної*** імплементації доданого до стегано-позиційного поліадичного числа елементу прихованого повідомлення. Це дозволяє в процесі стиснення відеосегменту забезпечити: маскування слідів вбудованої інформації; виключити вплив процесу імплементації інформації на достовірність значимих відеоресурсів, які використовуються в якості контейнерів.

Для заданої стеганографічної ємності за рахунок збільшення в 2,5 рази швидкості прихованого у послідовності кодованих ВС каналу передачі даних для розробленого методу відносно існуючих створюються умови для прихованої доставки в реальному часі інформації об'ємом: для швидкості каналу передачі даних 25 Мбіт/с- 30 % від Full HD (1920 × 1080).

ЛІТЕРАТУРА

[1] Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія. Київ: НАУ, 2013. 432 с.

[2] Ільяшов О. А., Бурячок В. Л. До питання захисту інформаційно-телекомунікаційної сфери від стороннього кібернетичного впливу. *Наука і оборона*. 2010. № 4. С. 35–41.

[3] Конахович Г. Ф., Пузиренко А. Ю. Комп'ютерна стеганографія. Теорія та практика. Київ : МК-Пресс, 2016. 288 с.

[4] Баранник В., Сидченко С., Баранник Д., Баранник В. Оцінка впливу недетермінованих характеристик на ефективність криптокомпресійного кодування зображень у диференційованому базисі. Безпека інформації. 2020. Т. 26, № 3. С. 168–180.

[5] Роман Одарченко, Максим Рябенко, Марина Іванова, Аль-Мудхафар Акіл Абдулхусейн М. Метод аналізу взаємодії параметрів qoe та qos на основі алгоритмів керування машинами. Наукоємні технології. 2022. № 4 (56). С. 305–316. DOI: https://doi.org/10.18372/2310-5461.56.17130.

[6] Krasnorutsky A., Onyshchenko R., Barannik D., Barannik V. The Methods of Intellectual Processing of Video Frames in Coding Systems in Progress Aeromonitor to Increase Efficiency and Semantic Integrity. 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022. P. 53–56. DOI: 10.1109/ATIT58178.2022.10024208.

[7] Козловський В. В., Савченко А. С., Толстікова О., Клобукова Л. Критерії вибору спектрально-ефективних сигналів у бездротових інформаційних мережах. *Наукоємні технології.* 2022. № 4 (56). С. 286–273. DOI: 10.18372/2310-5461.56.17125.

[8] Barannik V., Sidchenko S., Barannik D. Technology for protecting video information resources in the info-communication space. *Advanced Trends in Information Theory (ATIT 2020): Proceedings of IEEE 2nd International Conference.* Kyiv, 2020. P. 29–33.

[9] Задирака В. К., Никитенко Л. Л. Новые подходы к разработке алгоритмов скрытия информации. *Штучний інтелект.* 2008. № 4. С. 353–357.

[10] Barannik D., Barannik V., Korotin S., Bekirov A., Veselska O., Wieclaw L. Method of safety of informational resources on the basis of use of the indirect steganography. *Proceeding of the VIII International Conference of Students, PhD Students and Young Scientists.* Springer Nature Switzerland AG, 2020. Editors: S. Zawislak. Volume 70, ISSN 2211-0984. *Development of technology analysis for the content semantics* in *Engineer of XXI Century – We Design the Future*, Bielsko-Biała, Poland: ATH, 2020. P. 195–202. DOI: 10.1007/978-3-030-13321-4_17.

[11] Конахович Г. Ф. Оценка эффективности методов стеганографічного встраивания информации в спектральную область изображений. *АСУ та прилади автоматики*. 2014. Вип. 168. С. 23–29.

[12] Barannik D., Barannik V. Steganographic coding technology for hiding information in infocommunication systems of critical infrastructure. *2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT),* Kyiv, Ukraine, 2022, pp. 88–91. DOI: 10.1109/ATIT58178.2022.10024185.

[13] Information technology – JPEG 2000 image coding system: Secure JPEG 2000 [Text]. *International Standard ISO/IEC 15444-8, ITU-T Recommendation T.807.* 2007. 108 p.

[14] Задирака В. К., Кошкина Н. В., Никитенко Л. Л. Статистический анализ систем с цифровыми водяными знаками. *Штучний інтелект.* 2008. № 3. С. 315–324.

[15] Barannik V. et al. A method of scrambling for the system of cryptocompression of codograms service components. *In: Klymash, M., Luntovskyy, A., Beshley, M., Melnyk, I., Schill, A. (eds) Emerging Networking in the Digital Transformation Age. TCSET 2022. Lecture Notes in Electrical Engineering,* vol 965. Springer, Switzerland, Cham. DOI: 10.1007/978-3-031-24963-1_26.

[16] Баранник В. В., Баранник Д. В., Бекиров А. Є. Основи теорії структурно-комбінаторного стеганографічного кодування: монографія. Харків: Видавництво «Лідер», 2017. 256 с.

[17] Barannik V., Alimpiev A., Barannik D., Barannik N. Detections of sustainable areas for steganographic embedding. *East-West Design & Test Symposium (EWDTS).* IEEE, 2017. P. 555–558. DOI: 10.1109/EWDTS.2017.8110028.

[18] Бараннік Д. В. Метод двокаскадної імплантації прихованої інформації на основі стеганокомпресійних перетворень. *Інформаційні технології та електронна інженерія*. 2024. № 1. С. 31–38.

[19] Barannik V., Barannik D., Lekakh A. A steganographic method based on the modification of regions of the image with different saturation. *Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2018 14th International Conference on,* 2018, pp. 542–545. DOI: 10.1109/TCSET.2018.8336260.

[20] Бараннік Д. В. Технологія приховування інформативного контенту в динамічному потоці відеосегментів. *Наукоємні технології.* 2023. № 4. С. 408–415. DOI: 10.18372/2310-5461.60.18270.

Бараннік Д. В.

МЕТОД ЗМІШАНОГО СТЕГАНОКОМПРЕСІЙНОГО КОДУВАННЯ В ПОЗИЦІЙНО-ПОЛІАДИЧНОМУ БАЗИСІ

В статті обґрунтовується те, що досягнення відповідних вимог в процесі організації відеоінформаційного забезпечення та політики інформаційної безпеки є важливим аспектом досягнення ефективності управління критичною інфраструктурою. Тут потрібно враховувати те, що відеоінформаційні ресурси одночасно можуть мати два функціональних призначення, а саме як: значима інформація з позиції ключового впливу на ефективність аналізу та прийняття рішень в КРІС та ОСД; контейнерів для приховування спеціальних відомостей в системах комплексного захисту інформації. Показано актуальність та критичність забезпечення конфіденційності (спеціальної) інформації з використанням етапу формування та/або передачі бортовими інфокомунікаційними системами в умовах воєнного стану. Показано, що конфіденційність в загальному випадку може забезпечуватись комплексним підходом. Для цього залучаються технології криптографічного захисту та стеганографічних перетворень (СТП). Водночас збільшується актуальність та значимість застосування СТП. В той же час для сучасних варіантів сумісного послідовного використання стеганографічних та компресійних перетворень існують такі недоліки. Звідси існуючи методи СТП не забезпечують вимог за показниками: швидкості прихованого у кодованому відеопотоці каналу вбудованих повідомлень; стеганографічної ємності; обмеження впливу на ефективність компресійного кодування; цілісність вилученої на приймальній стороні прихованої інформації; демаскування факту наявності вбудованих до ВС прихованих повідомлень. Таким чином, мета досліджень статті полягає у необхідності підвищення ефективності стеганографічних перетворень в процесі передачі стиснутого (кодованого) відеопотоку інфокомунікаційними мережами для заданих властивостей відеосервісів з використанням бортових ІКС. Створено метод змішаного стеганокомпресійного

кодування на основі позиційно-поліадичного базису з маскуванням. Базові характеристики методу полягають у: створені стеганокомпресійних перетворень в змішано-маскованому базисі; реалізації двокаскадної ***кодово-компресійної*** *імплементації доданого до стегано-позиційного поліадичного числа елементу прихованого повідомлення.*

Ключові слова: стеганографічні перетворення, змішане стеганокомпресійне кодування, надмірність відеосегментів.

Barannik D.

METHOD OF MIXED STEGANOCOMPRESSION CODING IN POSITIONAL-POLYADIC BASIS

The article substantiates that the achievement of relevant requirements in the process of organizing video information support and information security policy is an important aspect of achieving the effectiveness of critical infrastructure management. Here it is necessary to take into account the fact that video information resources can simultaneously have two functional purposes, namely: significant information from the point of view of key influence on the effectiveness of analysis and decision-making in CRIS and DSS; containers for hiding special information in integrated information security systems. The relevance and criticality of ensuring the confidentiality of (special) information using the stage of formation and/or transmission by onboard infocommunication systems under martial law is shown. It is shown that confidentiality in the general case can be ensured by an integrated approach. For this, cryptographic protection and steganographic transformation (STT) technologies are involved. At the same time, the relevance and significance of the use of STT is increasing. At the same time, there are the following disadvantages for modern options for the combined sequential use of steganographic and compression transformations. Hence, the existing STT methods do not meet the requirements for the following indicators: the speed of the embedded message channel hidden in the encrypted video stream; steganographic container; limiting the impact on the effectiveness of compression coding; integrity of hidden information seized on the receiving side; unmasking the fact of the presence of hidden messages built into the aircraft. Thus, the purpose of the article is to increase the efficiency of steganographic transformations in the process of transmitting a compressed (encoded) video stream by infocommunication networks for the specified properties of video services using on-board ICS. A method of mixed steganocompression coding based on a positional-polyadic basis with masking has been created. The basic characteristics of the method are: created hip-compression transformations in a mixed-masked basis; implementation of two-stage code-compression implementation of the hidden message element added to the stegan-position polyadic number.

Keywords: steganographic conversions, mixed steganocompression coding, redundancy of video segments.

Стаття надійшла до редакції 01.11.2024 р.
Прийнято до друку 11.12.2024 р.